February 23, 2006

Information Technology Management

DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements
(D-2006-052)

Department of Defense
Office of Inspector General

Quality   *Integrity*   *Accountability*

Report Documentation Page

1. REPORT DATE **23 FEB 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Management: DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
ODIG-AUD (ATTN: AFTS Audit Suggestions),Inspector General of the Department of Defense,400 Army Navy Drive (Room 801),Arlington,VA,22202-4704	

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**35**	

Acronyms

AEFC	Air and Space Expeditionary Force Center
CIO	Chief Information Officer
DoD IG	Department of Defense Inspector General
ESA	Enterprise Service Activity
COR	Contracting Officer's Representative
GAO	Government Accountability Office
IA	Information Assurance
IT	Information Technology
JPAS	Joint Personnel Adjudication System
MIPR	Military Interdepartmental Purchase Request
NETC	Naval Education and Training Command
SPAWARSYSCOM	Space and Naval Warfare Systems Command
SSC	Space and Naval Warfare Systems Center
USARC	U.S. Army Reserve Command

February 23, 2006

MEMORANDUM FOR ASSISTANT SECRETARY OF THE AIR FORCE FOR
FINANCIAL MANAGEMENT AND COMPTROLLER
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Report on DoD Organization Information Assurance Management of
Information Technology Goods and Services Acquired Through Interagency
Agreements (Report No. D-2006-052)

We are providing this report for review and comment. We considered
management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly.
The Space and Naval Warfare Systems Command comments were not responsive. We
request additional comments on Recommendations 2.a. and 2.b. Additionally, the
U.S. Army Reserve Command commented on the findings, but did not provide comments
on Recommendation 1. We ask that both organizations provide comments addressing
these recommendations by April 24, 2006.

If possible, please send management comments in electronic format (Adobe
Acrobat file only) to AudATM@dodig.mil. Copies of the management comments must
contain the actual signature of the authorizing official. We cannot accept the / Signed /
symbol in place of the actual signature. If you arrange to send classified comments
electronically, they must be sent over the SECRET Internet Protocol Router Network
(SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed
to Ms. Jacqueline L. Wicecarver at (703) 604-9077 (DSN 664-9077) or Ms. Therese M.
Kince at (703) 604-9060 (DSN 664-9060). The team members are listed inside the back
cover. See Appendix C for the report distribution.

By direction of the Deputy Inspector General for Auditing:

Richard B. Jolliffe
Assistant Inspector General
Acquisition and Contract Management

Department of Defense Office of Inspector General

Report Number D-2006-052   February 23, 2006
(Project No. D2005-D000AS-0173)

DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements

Executive Summary

Who Should Read This Report and Why? Chief information officers within DoD and individuals responsible for DoD Component information assurance should read this report because it contains information on properly securing information technology goods and services purchased through interagency agreements.

Background. Many Federal agencies, including DoD, are now making greater use of interagency agreements to improve the Government's aggregate buying power and simplify the procurement process. The information technology goods and services purchased through these agreements do not stand alone, but instead are part of the seamless web of communications networks, computers, software, databases, applications, security services, and other capabilities used by DoD. As a result, information assurance is an important aspect of any DoD information system, no matter how the system components or services are acquired, whether through traditional acquisitions or interagency agreements.

DoD Components are required to implement and maintain adequate security programs that include the minimum information assurance controls outlined in DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, for all DoD information systems. Army, Navy, and Air Force chief information officers rely on subordinate command chief information officers to follow this guidance for all information systems, including those acquired through interagency agreements. Additionally, the National Institute of Standards and Technology Special Publication 800-12, "An Introduction to Computer Security," October 1995, recommends monitoring procedures for tracking user activity on DoD systems and networks.

Results. Officials at four DoD organizations within the Army, Navy, and Air Force did not fully implement comprehensive information assurance controls required to protect DoD information. Specifically, organization users were granted access to DoD systems prior to receiving information assurance training, user security clearances were not verified, and user activity reviews were not conducted. As a result, the integrity, confidentiality, and availability of DoD operational data and information technology systems cannot be guaranteed. See the Finding section of the report for the detailed recommendations. The U.S. Army Reserve Command and Space and Naval Warfare Systems Command (including the Space and Naval Warfare Systems Center San Diego) management controls for coordinating, documenting, and tracking information assurance training completion were not adequate to ensure that training was provided to all personnel and the management controls for verifying user security clearances were not

adequate to ensure that access was granted to the appropriate personnel. The Air and Space Expeditionary Force Center management controls for monitoring user activity were not adequate to detect, report, and document attempted or realized penetrations of information systems. Implementing the recommendations will correct the identified weaknesses.

Management Comments and Audit Response. The Commander, U.S. Army Reserve Command responded to the findings in the draft of this report, but did not respond to the recommendations. The U.S. Army Reserve Command should provide comments on the final report by April 24, 2006. The Commander, Space and Naval Warfare Systems Command and the Commander, Space and Naval Warfare Systems Center San Diego concurred with two of the recommendations and were not responsive to two of the recommendations. We do not agree that there is a clear procedure for ensuring that information assurance awareness training is properly documented and tracked for all personnel. The Commander, Air and Space Expeditionary Force Center concurred with the recommendations; therefore no further comments are required. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Background

Interagency Agreements. Many Federal agencies are now making greater use of interagency agreements to purchase commonly used goods[1] and services,[2] including information technology (IT), thereby improving the Government's aggregate buying power and simplifying the procurement process. The IT goods and services purchased through these agreements do not stand alone, but instead are part of the DoD communications networks, computers, software, databases, applications, and security services. Information assurance (IA) is an important aspect of all DoD information systems, no matter how the system components or services are acquired, whether through traditional acquisitions or interagency agreements.

Information Assurance. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, states that each DoD Component is responsible for implementing and maintaining an adequate security program for information and IT assets that includes an IA architecture, a supporting master plan, clear assignment of organizational roles and responsibilities, and for developing and managing a professional IA workforce.

Command Roles and Responsibilities. DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002, certified current as of November 21, 2003, directs the Assistant Secretary of Defense for Networks and Information Integration, as the DoD Chief Information Officer (CIO), to monitor and evaluate IA by developing guidance and annually evaluating DoD Component readiness. Further, DoD Directive 8500.1 requires DoD Component heads to develop and implement Component-specific IA programs and provide IA awareness training to all Component personnel. Army, Navy, and Air Force CIOs rely on subordinate organization CIOs to follow this guidance for all information systems, including those acquired through interagency agreements. As such, we focused on IA policy and guidance implementation at several Army, Navy, and Air Force organizations to assess the overall effectiveness of the DoD and Service CIO management of IA controls over IT goods and services obtained through interagency agreements. DoD Instruction 8500.2 establishes a baseline IA level for all DoD information systems through the assignment of specific IA controls.

Information Assurance Controls. IA controls protect and defend the integrity, confidentiality, and availability of information and information systems and include user IA awareness training, security clearance documentation, and user activity monitoring.

This report will focus on IA controls for four of the six interagency purchases selected:

- U.S. Army Reserve Command (USARC) used Military
  Interdepartmental Purchase Request (MIPR) No. MIPR04CIBER037

---

[1]Goods are tangible products, such as computer hardware or software.

[2]Services are work performed by a contractor to update, implement, or change an already established system, such as systems integration or administrative tasks.

to pay the balance owed on an existing interagency agreement, allowing the command to rebid for network services using traditional acquisition processes.

- Space and Naval Warfare Systems Command (SPAWARSYSCOM), used MIPR No. N0003904IPFLD36 to purchase a systems integration to ensure that communications and advanced command hardware meet requirements.

- Naval Education and Training Command (NETC) used MIPR No. N6804504MPAC202 to fund the procurement and installation of 5,000 computer workstations, including physical connections, network configuration, de-installation, on-site data wiping, and disposal/decommissioning of existing computers.

- Air and Space Expeditionary Force Center (AEFC) used MIPRs No. DD44809N401228 and DD44809N401229 to purchase on-site Continuity of Operations equipment and off-site backup equipment.

Objectives

Our overall audit objective was to evaluate DoD and Service CIO processes for managing IT goods and services obtained through interagency agreements and determine whether those processes adequately addressed information security. Specifically, we determined whether DoD and Service CIOs followed DoD and Federal policies for proper certification and accreditation, risk assessment, and user access permissions related to DoD information systems. We also reviewed the managers' internal control program as it related to the overall objective. See Appendix A for a discussion of the scope and methodology and Appendix B for prior coverage related to the objectives.

Managers' Internal Control Program

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Managers' Internal Control Program. We reviewed the adequacy of management controls over DoD Component IT resources. Specifically, we reviewed USARC, SPAWARSYSCOM and Space and Naval Warfare Systems Center (SSC) San Diego, NETC, and AEFC management controls over IT funding and IA. In addition, we reviewed management's self-evaluation applicable to those controls.

Adequacy of Management Controls. We reviewed material management control weaknesses for the four sites visited, as defined by DoD Instruction 5010.40. The USARC, SPAWARSYSCOM, and SSC San Diego management controls for coordinating, documenting, and tracking IA training completion were not adequate to ensure that training was provided to all personnel in accordance with DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004. The USARC, SPAWARSYSCOM, and SSC San Diego management controls for verifying user security clearances were not adequate to ensure that access was granted to the appropriate personnel in accordance with the Office of Management and Budget Circular A-130, "Security of Federal Automated Information Resources," November 28, 2000, and the Office of the Under Secretary of Defense Memorandum, "Facilitating Classified Visits within the Department of Defense," April 1, 2005. The AEFC management controls for monitoring user activity were not adequate to detect, report, and document attempted or realized penetrations of information systems because the procedures for doing so were not documented. Implementing the recommendations will correct the identified weaknesses. A copy of the report will be provided to the senior officials responsible for management controls at USARC, SPAWARSYSCOM, and AEFC. We did not identify any management control weaknesses at NETC.

Adequacy of Management's Self-Evaluation. USARC officials did not identify IA as an assessable unit and, therefore, did not identify or report the management control weaknesses identified by our audit. Program Executive Officer Command, Control, Communications, Computers and Intelligence and Space officials identified IA accreditation as part of an assessable unit but did not perform an evaluation because management did not complete the schedule in the management control plan. AEFC officials identified IT as an assessable unit; however, during its evaluation they did not identify the management control weaknesses identified by this audit because the AEFC evaluation covered a much broader area. NETC officials identified IA as an assessable unit and, like the audit team, identified no specific management control weakness related to the unit.

DoD Organization Information Assurance Management

Officials at four DoD organizations within the Army, Navy, and Air Force had not fully implemented the comprehensive IA controls that are required to protect DoD information systems. Specifically:

- organization users did not receive IA awareness training prior to being granted access to DoD systems,

- user security clearances were not verified, and

- user activity reviews were not conducted.

DoD organization officials did not fully implement IA controls because IA roles and responsibilities were unclear and current operations were not documented. As a result, the integrity, confidentiality, and availability of DoD operational data and IT systems cannot be guaranteed.

Information Assurance Controls

Officials at four DoD organizations within the Army, Navy, and Air Force had not fully implemented comprehensive IA controls that are required to protect DoD information systems. DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002, certified current as of November 21, 2003, assigns responsibility to DoD Component Heads for developing and implementing IA programs focused on securing the integrity, confidentiality, and availability of DoD information and information systems. Instead, DoD Components rely on organization-level CIOs to develop and fully implement tailored, comprehensive IA programs for all IT goods and services obtained, whether through traditional acquisitions or interagency agreements.

Information Assurance Awareness Training. DoD Directive 8570.1 "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, requires that all authorized users, including contractors, receive IA awareness training as a condition of access to any DoD system and, thereafter, complete annual IA refresher training.

From May through August 2005, we included in our USARC selection for review any Government or contract official with access to or responsibility for the existing interagency agreement that was paid-in-full using MIPR No. MIPR04CIBER037. Additionally, from June through August 2005, we included in our SPAWARSYSCOM and SSC San Diego selection for review any Government or contract official with access to or responsibility for the systems integration using MIPR No. N0003904IPFLD36.

USARC and SPAWARSYSCOM, and SSC San Diego system users did not receive IA awareness training prior to being granted access to the systems because USARC, SPAWARSYSCOM, and SSC San Diego officials did not

4

effectively coordinate, document, and track IA training for all personnel and IT users.

USARC officials could not provide completed training forms for 8 of the 15 contractor personnel (53 percent) reviewed because USARC Headquarters and USARC Enterprise Service Activity (ESA) personnel did not clearly establish who was responsible for retaining IA training records and verifying completion. USARC Headquarters and USARC ESA officials should identify and assign specific roles and responsibilities for implementing the USARC IA awareness training program.

SPAWARSYSCOM and SSC San Diego officials could not provide IA training documents for any of the seven contract personnel reviewed because officials did not clearly establish responsibility for ensuring that IA training was completed by all personnel, including contractors. SPAWARSYSCOM and SSC San Diego officials should identify and assign specific roles and responsibilities for implementing the SPAWARSYSCOM and SSC San Diego IA awareness training program.

USARC, SPAWARSYSCOM, and SSC San Diego personnel should improve their IA awareness training programs for all employees and contractors so that all Government and contract personnel are aware of their security roles and responsibilities and understand the potential threats to DoD systems before they gain access to information systems.

User Access Controls. DoD organization officials did not adequately verify user security clearances or conduct user activity reviews.

> **User Security Clearances.** The Office of Management and Budget Circular A-130, "Security of Federal Automated Information Resources," November 28, 2000, requires that individual security clearances be verified prior to authorizing personnel access to IT systems, and periodically thereafter. Further, the Office of the Under Secretary of Defense Memorandum, "Facilitating Classified Visits within the Department of Defense," April 1, 2005, requires that the Joint Personnel Adjudication System (JPAS) be used to verify personnel security clearances for visitors requiring access to classified information.

The four DoD organizations reviewed had developed procedures for verifying the identity, personnel security clearance, and need-to-know for all visitors prior to giving authorized access to IT systems. However, two of the four organizations, USARC and SPAWARSYSCOM, did not fully implement the procedures developed and, as a result, were not adequately verifying user security clearances.

> USARC Headquarters and USARC ESA officials did not clearly establish responsibility for user security clearance verification. For example, USARC ESA and USARC Headquarters officials could not provide JPAS security verification for 6 of the 15 contractors reviewed. USARC officials provided visit authorizations for some users and JPAS verifications for others. Not only was there confusion regarding which officials were responsible for verifying which users, but also regarding the required documents and procedures to be used.

USARC officials should identify and assign specific roles and responsibilities for verifying USARC user security clearances.

Although SPAWARSYSCOM and SSC San Diego officials verified contract agency facility clearances[3] by confirming that each visit request was necessary, they did not adequately verify that individual security clearances[4] were current, nor did they validate each using JPAS because the procedures were unclear and not documented. This current process fully relies on the contract agency to provide accurate information on individual contractors who may change during the course of a project. SPAWARSYSCOM and SSC San Diego officials should define specific responsibilities for verifying individual security clearance information and use the JPAS to validate individual clearance information.

User Activity Reviews. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, requires that DoD Component IA programs detect, report, and document attempted or realized penetrations of DoD information systems and include appropriate countermeasures or corrective actions. The National Institute of Standards and Technology Special Publication 800-12, "An Introduction to Computer Security," October 1995, recommends periodic monitoring of audit logs to identify unauthorized use.

While three of the four DoD organizations reviewed had developed user activity monitoring programs to protect their systems, AEFC did not fully implement a user activity monitoring program because specific procedures were not documented and a formal, recurring monitoring schedule had not been developed. Instead, AEFC officials stated they informally review the audit logs three times a week for suspicious activity. These procedures rely on infinite permanency in personnel positions and consistent memory to periodically review the logs. AEFC officials should develop standard written procedures for monitoring user activity and establish a schedule for reviewing system audit logs that will help protect organization information and IT systems. Without such a monitoring system, the AEFC organization systems' first line of defense may be weakened.

Conclusion

The integrity, confidentiality, and availability of DoD operational data and IT systems cannot be guaranteed because IA awareness training programs were not fully implemented and monitored, user security clearances were not adequately verified, and user activity reviews were not conducted regularly. Without proper training implementation and recording, the integrity of DoD systems cannot be guaranteed because users may not be aware of, and strictly adhere to, the standards of conduct necessary to protect the information. Additionally, if user

---

[3]Facility clearances are granted to an entire contractor facility, based on an investigation verifying that the individuals who run, own, and manage the facility have been cleared.

[4]Individual security clearances are granted to individual personnel, based on background investigations and personal interviews.

security clearances are not adequately verified, then the confidentiality of secretly disclosed or closely held organization information may be compromised because the information may be released to individuals who are not properly cleared. Furthermore, if user activity reviews are not conducted regularly, users may improperly use organization systems to damage or impair the availability of critical DoD information.

Previous DoD Inspector General (DoD IG) Report No. D2005-025, "DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness," December 17, 2004, identified weaknesses in IA training programs at the Defense Commissary Agency, Defense Contract Management Agency, and Washington Headquarters Services. The report concluded that the DoD CIO did not establish adequate procedures for DoD Components to monitor IA awareness training. Our report identifies similar weaknesses at USARC, SPAWARSYSCOM, and SSC San Diego. Our repeated identification of systemic IA training weaknesses at various DoD activities indicates that the DoD CIO and individual DoD Components continue to ineffectively monitor and implement their IA training programs. No additional recommendations to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer will be made at this time because ongoing corrective actions for the recommendations made in DoD IG Report No. D2005-025 should correct the identified problems.

Management Comments on the Findings and Audit Response

Management Comments. The Commander, U.S. Army Reserve Command stated that the findings and recommendations in the draft report were incorrect or were no longer valid concerns. The Commander, U.S. Army Reserve Command stated that MIPR No. MIP04CIBER037 expired in September 2004 and a new contract with a different contractor was in place at USARC as of July 2005.

Audit Response. USARC comments were not responsive. The audit team focused on contract personnel that were retained by the new contract. DoD information assurance policies and procedures apply to the new contract and contractor.

Information Assurance Awareness Training. The Commander, U.S. Army Reserve Command stated that USARC has an IA training program in place which includes both initial IA training (provided in a Newcomer's Orientation) and annual refresher training (provided via Web-based instruction). Further, the Commander, U.S. Army Reserve Command stated that the USARC Information Assurance Security Officer maintains training certificates for those who complete IA training in a centralized database. Finally, the Contracting Officer's Representative (COR) and the Contractor's Program Manager, who were not interviewed during the site visit, maintain IA training records for contract personnel.

Audit Response. USARC comments were not responsive. DoD Directive 8570.1 requires that IA training be tracked and documentation be maintained by the IA Security Officer. However, the IA Security Officer had not tracked or documented that the reviewed contractor personnel had received training. Additionally, the IA Security Officer did not provide information or an agreement that either the COR or the Contractor's Program Manager were designated with the responsibility to track and document IA training. Therefore, USARC could not provide assurance that contractor personnel received the required IA training before accessing DoD information systems.

User Security Clearances. The Commander, U.S. Army Reserve Command stated that USARC Headquarters G-2/6 Security Office was responsible for verifying security clearance information and has used JPAS for more than 2 years. Additionally, the Commander, U.S. Army Reserve Command stated that the USARC G-2/6 Security Office assigned security managers within every directorate, both Headquarters and the USARC ESA. Further, USARC stated that the COR and the Contractor's Program Manager maintain contractors' security clearance information.

Audit Response. USARC comments were not responsive. Neither USARC Headquarters G-2/6 Security Office nor USARC ESA Security Managers could provide documentation that verified contractors maintained the proper security clearances. It is the responsibility of the IA security office to verify and maintain documentation that contractors' security clearances are valid and updated.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Commander, U.S. Army Reserve Command direct the Chief Information Officer, U.S. Army Reserve Command to:

a. Conduct and document annual information assurance awareness training, in accordance with DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, for all U.S. Army Reserve Command employees and contractors.

b. Within 30 days of report issuance, establish clear procedures that designate organization-specific roles and responsibilities for tracking training for all employees and contractors.

c. Within 30 days of report issuance, establish clear procedures designating specific roles and responsibilities for verifying individual security clearances in accordance with the Office of Management and Budget Circular A-130, "Security of Federal Automated Information Resources," November 28, 2000, for all U.S. Army Reserve Command employees and contractors.

Management Comments. The Commander, U.S. Army Reserve Command did not comment on the recommendations. We request the Commander, U.S. Army

Reserve Command provide comments to the final report recommendations by April 24, 2006.

2. We recommend that the Commander, Space and Naval Warfare Systems Command direct the Chief Information Officer, Space and Naval Warfare Systems Command and the Chief Information Officer, Space and Naval Warfare Systems Center San Diego to:

a. Conduct and document annual information assurance awareness training, in accordance with DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, for all Space and Naval Warfare Systems Command employees and contractors.

Management Comments. The Commander, Space and Naval Warfare Systems Command concurred with Recommendation 2.a. The Commander, Space and Naval Warfare Systems Command stated that IA training is conducted and documented for all personnel to include contractors with computer system and network access. The Commander, Space and Naval Warfare Systems Command works within the Navy-Marine Corps Intranet network. IA training was conducted command-wide in FY 2005 and a manual process is in place to track completion of IA training. Individuals are responsible to provide completion certificates to the Command IA Manager. Additionally, new personnel who require access to the Navy-Marine Corps Intranet must compete IA training and provide a certificate prior to receiving access approval. SSC San Diego conducts and documents IA training for all military, Government, and contractor personnel with computer system and network access. SSC San Diego has established a Web-based training module that automatically updates and tracks training. Center-wide IA training was completed on September 30, 2005.

Audit Response. Although the Commander, Space and Naval Warfare Systems Command concurred with the recommendation, the comments were not responsive. SPAWARSYSCOM and SSC San Diego were unable to provide training documentation for the contractors reviewed that showed they had received the required IA training before accessing the DoD information system. The SPAWARSYSCOM current system does not ensure that personnel who are outside the Navy-Marine Corps Intranet network will receive IA training as required by DoD Directive 8570.1.

b. Within 30 days of report issuance, establish clear procedures designating organization-specific roles and responsibilities for tracking training for all employees and contractors.

Management Comments. The Commander, Space and Naval Warfare Systems Command responded stating that SPAWARSYSCOM and SSC San Diego already have a clear procedure in place to track training for all personnel. Information Assurance Managers for each system center within the claimancy are appointed in writing and are responsible for ensuring training of individuals with access to their networks. SPAWARSYSCOM Claimancy IA staff including SSC San Diego provides metrics to the Claimant IA Program Manager on a monthly basis, and holds monthly and quarterly program reviews where they address progress on key areas such as compliance with training.

Audit Response. SPAWARSYSCOM and SSC San Diego comments were not responsive. Neither SPAWARSYSCOM nor SSC San Diego officials could identify individual roles and responsibilities to track training of all personnel including the contractors reviewed. Specifically, employees within the SPAWARSYSCOM Claimancy IA staff were unable to identify the individual responsible for tracking the IA training of the seven contract personnel. These contractors had access to DoD information systems before receiving the required IA training outlined in DoD Directive 8570.1. Therefore, SPAWARSYSCOM and SSC San Diego officials cannot be assured that personnel who have not received IA training before being granted access to DoD information systems are aware of their security roles and responsibilities and understand the potential threats to DoD systems.

c. Within 30 days of report issuance, establish clear procedures designating specific roles and responsibilities for verifying individual security clearances in accordance with the Office of Management and Budget Circular A-130, "Security of Federal Automated Information Resources," November 28, 2000, for all Space and Naval Warfare Systems Command employees and contractors.

d. Begin using the Joint Personnel Adjudication System immediately to validate individual security clearances in accordance with the Office of the Under Secretary of Defense Memorandum, "Facilitating Classified Visits within the Department of Defense," April 1, 2005.

Management Comments. SPAWARSYSCOM concurred with Recommendations 2.c. and 2.d. stating that SPAWARSYSCOM will develop a policy directive covering SPAWARSYSCOM claimancy and supported Program Executive Offices, which will establish procedures for verifying individual personnel security clearances and identify specific roles and responsibilities. SPAWARSYSCOM estimates completion for Recommendation 2.c. by June 30, 2006. Further, SPAWARSYSCOM and SSC San Diego are in the process of implementing the JPAS for the verification of security clearances. Additionally, a Security Functional Change Lead Team will establish a new security policy directive/manual that will comply with Office of the Under Secretary of Defense Memorandum and Chief of Naval Operations policy to ensure visitor and security clearance information is verified prior to authorizing access to SPAWARSYSCOM facilities and classified information. The estimated completion is April 1, 2006.

3. We recommend that the Commander, Air and Space Expeditionary Force Center direct the Systems Administrator, Air and Space Expeditionary Force Center to:

a. Deactivate inactive, suspended, and terminated accounts immediately.

b. Review audit logs for failed and unauthorized user attempts to log in.

c. Document consistent procedures that will help to implement the deactivation of inactive, suspended, and terminated accounts and establish a schedule to review audit logs on no less than a weekly basis for failed and unauthorized user attempts to log in.

Management Comments. The Commander, Air and Space Expeditionary Force Center concurred and ordered that all inactive, suspended, or terminated accounts be deactivated immediately, effective January 13, 2006. Additionally, the Air Force response stated that the AEFC Commander ordered reviews of all system access logs under the control of AEFC to be performed and annotated in a System Information Assurance Log on a weekly basis, effective January 11, 2006. Finally, the Air Force response stated that the AEFC Commander ordered development of permanent policy and procedures that address monitoring user activity and established a schedule for reviewing system access on a weekly basis. According to the Air Force response, policy documentation is due to the AEFC Commander for review and approval by February 15, 2006.

Appendix A. Scope and Methodology

We met with DoD Office of Inspector General, Contract Management officials to gather information regarding their project, "Audit of DoD Purchases Through the General Service Administration," (Project No. D2004-D000CF-0238.000). From these meetings we obtained and reviewed documentation and working papers to identify IT goods and services worth at least $100,000 that were purchased through interagency agreements. We selected the following eight MIPRs used by six DoD organizations for review:

- USARC used MIPR No. MIPR04CIBER037 to pay the balance ($2,135,811) on an existing interagency agreement, allowing the command to re-bid for Army Reserve Network services using traditional acquisition processes.

- SPAWARSYSCOM used MIPR No. N0003904IPFLD36 to purchase a $1,699,021 systems integration to ensure that communications and advanced command hardware meet requirements.

- NETC used MIPR No. N6804504MPAC202 to fund an $8,000,000 procurement and installation for 5,000 computer workstations at 33 sites, including physical connections, network configuration, de-installation, on-site data wiping, and disposal/decommissioning.

- AEFC used MIPRs No. DD44809N401228 and DD44809N401229 to purchase on-site Continuity of Operations equipment for $40,143 and off-site backup equipment for $172,246.

- Commander, Naval Reserve Forces Command used MIPR No. N0007204MP34275 to procure Defense Message System equipment valued at $706,324.

- U.S. Southern Command used MIPRs No. MIPR4F21K60065 and MIPR4M21T60129 to purchase software integration and technical services totaling $7,500,000 for the Logistics Command and Control System in Colombia. However, we did not visit U.S. Southern Command in Miami, Florida, because all documents, hardware, and software related to MIPRs No. MIPR4F21K60065 and MIPR4M21T60129 at the U.S. Southern Command were controlled by the Colombian government, and therefore outside of our scope.

We met with the DoD and Service CIOs to gather information regarding their management of interagency agreements, specifically our selected purchases, and identify the implemented IA requirements for each Service. Additionally, we met with Security officials from the DoD Office of Inspector General to identify information security procedures.

We reviewed Federal and DoD policy to identify the procedures established for DoD Component IA programs, including IA training, user access, certification

and accreditation, and risk assessment. Specifically, we reviewed DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002, certified current as of November 21, 2003, to gather overall IA requirement information and determine DoD Component heads' roles and responsibilities for IA programs.

Information Assurance Training. We reviewed DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, to identify IA training requirements for DoD employees and contractors.

User Security Clearance Verification. We reviewed the Office of Management and Budget Circular A-130, "Security of Federal Automated Information Resources," November 28, 2000, to determine existing requirements for verifying individual security clearances prior to providing authorized access to DoD systems. Additionally, we reviewed the Office of the Under Secretary of Defense Memorandum, "Facilitating Classified Visits within the Department of Defense," April 1, 2005, which better defines the required security clearance verification system to be used.

User Activity Monitoring. We reviewed DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and the National Institute of Standards and Technology Special Publication 800-12, "An Introduction to Computer Security," October 1995, to determine the recommended monitoring procedures for tracking user activity on DoD systems and networks.

We conducted interviews with IA, system administration, security, and certification and accreditation officials at the following sites to gather detailed information on the IA procedures each DoD Component developed and implemented, related to the six selected MIPRs:

- USARC in Fort McPherson, Georgia, and USARC ESA in Peachtree City, Georgia;

- SPAWARSYSCOM Headquarters and SPAWAR Systems Center in San Diego, California;

- NETC Headquarters, Naval Air Station Pensacola and the Center for Naval Leadership, Naval Base Corry Station in Pensacola, Florida; Aegis Training and Readiness Center, Naval Surface Warfare Center Dahlgren Division in Dahlgren, Virginia; Navy-Marine Corps Intelligence Training Center in Virginia Beach, Virginia; and the Center for Naval Aviation Technical Training Unit, Naval Air Station Oceana in Virginia Beach, Virginia;

- AEFC at Langley Air Force Base in Virginia; and

- Commander, Naval Reserve Forces Command in New Orleans, Louisiana.

Additionally, we identified some conditions during our site visit at the Commander, Naval Reserve Forces Command but, due to the condition of the

New Orleans area after Hurricane Katrina, no recommendations will be forthcoming.

During our interviews with the identified officials, we reviewed system security authorization agreements; training completion documents; security clearance verification forms; computer audit logs; and standard operating procedures related to IA training, user security clearances, and user activity monitoring to determine whether DoD Components properly followed Federal and DoD guidance. Additionally, we used judgmental samples of personnel involved with the IT goods or services purchased to test whether each Component's user access procedures were in accordance with applicable laws.

We performed this audit from April 2005 through December 2005 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We relied on computer-processed event or audit logs generated by the DoD Component information systems. We reviewed the information in the event or audit logs for compliance with Federal and DoD guidance, but we did not assess the validity or accuracy of the systems used by the DoD Components to generate the data.

Government Accountability Office High-Risk Area. The Government Accountability Office (GAO) has identified several high-risk areas in DoD. This report provides coverage of the Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures high-risk areas.

Appendix B. Prior Coverage

During the last 5 years, GAO, DoD IG, the Army Audit Agency, the Naval Audit Service, and the Air Force Audit Agency have issued 12 reports discussing information assurance. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-05-362, "Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk," April 22, 2005

GAO Report No. GAO-01-307, "Progress and Challenges to an Effective Defense-wide Information Assurance Program," March 30, 2001

DoD IG

DoD IG Report No. D-2005-096, "DoD Purchases Made Through the General Services Administration," July 29, 2005

DoD IG Report No. D-2005-094, "Proposed DoD Information Assurance Certification and Accreditation Process," July 21, 2005

DoD IG Report No. D-2005-054, "DoD Information Technology Security Certification and Accreditation Process," April 28, 2005

DoD IG Report No. D-2005-025, "DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness," December 17, 2004

Army Audit Agency

Army Audit Agency Report No. A2004-0216-FFB, "Information Systems Security Material Weakness," April 8, 2004

Naval Audit Service

Naval Audit Service Report No. N2004-0072, "Operational Controls at Naval Air Systems Command Headquarters and Naval Air Warfare Centers," August 16, 2004

Naval Audit Service Report No. N2004-0063, "Operational Controls at Naval Aviation Depots," July 9, 2004

Naval Audit Service Report No. N2004-008, "Information Technology Certification and Accreditation Process," October 28, 2003

Air Force Audit Agency

Air Force Audit Agency Report No. F2005-0002-FB4000, "Information Assurance Position Certification Training for Air Force Network Professionals," March 21, 2005

Air Force Audit Agency Report No. F2002-0003-C06600, "Certification and Accreditation of Air Force Systems," April 22, 2002

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense for Networks and Information Integration/DoD Chief
    Information Officer
Chief Information Officer, Office of the Secretary of Defense
Director, Program Analysis and Evaluation
Director, Defense Procurement and Acquisition Policy

Joint Staff

Director, Joint Staff
Chief Information Officer, Joint Staff

Department of the Army

Assistant Secretary of the Army for Financial Management and Comptroller
Auditor General, Department of the Army
Chief Information Officer, Department of the Army
Commander, U.S. Army Reserve Command

Department of the Navy

Assistant Secretary of the Navy for Manpower and Reserve Affairs
Naval Inspector General
Auditor General, Department of the Navy
Chief Information Officer, Department of the Navy
Commander, Space and Naval Warfare Systems Command
Commander, Space and Naval Warfare Systems Center San Diego

Department of the Air Force

Assistant Secretary of the Air Force for Financial Management and Comptroller
Auditor General, Department of the Air Force
Chief Information Officer, Department of the Air Force
Commander, Air and Space Expeditionary Force Center

Unified Commands

Chief Information Officer, U.S. Northern Command
Chief Information Officer, U.S. Southern Command
Chief Information Officer, U.S. Joint Forces Command
Chief Information Officer, U.S. Pacific Command
Chief Information Officer, U.S. European Command
Chief Information Officer, U.S. Central Command
Chief Information Officer, U.S. Transportation Command
Chief Information Officer, U.S. Special Operations Command
Chief Information Officer, U.S. Strategic Command

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Department of the Army Comments

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY RESERVE COMMAND
1401 DESHLER STREET SW
FORT MCPHERSON, GA 30330-2000

REPLY TO
ATTENTION OF

AFRC-CII

2 February 2006

MEMORANDUM FOR Program Director, Acquisition and Technology Management, Inspector General, Department of Defense, 400 Army Navy Drive, Arlington, VA 22202-4704

SUBJECT: Report on DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements (Project No. D2005-D000AS-0173)

1. Reference Draft Report, Program Director, Acquisition and Technology Management, Inspector General, January 6, 2006, subject as above.

2. The Draft Report, referenced above, was focused on an interagency purchase, Military Interdepartmental Purchase Request (MIPR) No. MIPR04CIBER037, that had expired in September 2004. At the time of the audit, there was a different contract and contractor on site. The on site Contracting Officer's Representative (COR) was not interviewed by the audit team. The findings and recommendations presented in this report are incorrect, or no longer valid concerns.

3. Under Information Assurance Awareness Training, the Draft Report states –

    a. USARC system users did not receive IA awareness training prior to being granted access to the systems because USARC officials did not effectively coordinate, document, and track IA training for all personnel and IT users.

    b. USARC officials could not provide completed training forms for 8 of the 15 contractor personnel (53 percent) reviewed because USARC Headquarters and USARC Enterprise Service Activity (ESA) personnel did not clearly establish who was responsible for retaining IA training records and verifying completion. USARC Headquarters and USARC ESA officials should identify and assign specific roles and responsibilities for implementing the USARC IA awareness training program.

    c. USARC personnel should improve their IA awareness training programs for all employees and contractors so that all Government and contract personnel are aware of their security roles and responsibilities and understand the potential threats to DoD systems before they gain access to information systems.

AFRC-CII
SUBJECT: Report on DoD Organization Information Assurance Management of
Information Technology Goods and Services Acquired Through Interagency
Agreements (Project No. D2005-D000AS-0173)

4. Under User Security Clearances, the Draft Report states –

   a. The DoD organizations reviewed had developed procedures for verifying
the identity, personnel security clearance, and need-to-know for all visitors prior
to giving authorized access to IT systems. However, USARC did not fully
implement the procedures developed and, as a result, were not adequately
verifying user security clearances.

   b. USARC Headquarters and USARC ESA officials did not clearly establish
responsibility for user security clearance verification. For example, USARC ESA
and USARC Headquarters officials could not provide Joint Personnel
Adjudication System (JPAS) security verification for 6 of the 15 contractors
reviewed. USARC officials provided visit authorizations for some users and Joint
Personnel Adjudication System verifications for others. Not only was there
confusion regarding which officials were responsible for verifying which users,
but also regarding the required documents and procedures to be used. USARC
officials should identify and assign specific roles and responsibilities for
verifying USARC user security clearances.

5. In response to your findings referenced in paragraph 3 (Information Assurance
Awareness Training), the USARC does have an IA training and awareness
program in place. As newly assigned personnel arrive within the USARC, they
are sent through the Newcomers Orientation in which IA user awareness is part
of its program of instruction. Annually all users are required to take Web-based
IA awareness training from one of two published locations. Once a user
completes the required training, that certification is maintained by the Information
Assurance Security Officer within a centralized data base. In addition,
contractors IA training certification is maintained by the COR and the
Contractor's Program Manager. But to reiterate, the COR was not interviewed by
the auditing team.

6. In response to your findings referenced in paragraph 4 (User Security
Clearances), the USARC Headquarters G-2/6 Security Office has had the
responsibility of security clearance verification since the Command was started.
The USARC G-2/6 Security Office also has assigned Security Managers within
every directorate, at the Headquarters and at USARC ESA. The Security Office
has also been using the JPAS system in excess of two years. There has never
been a question within the command as to who validates security clearances. In
addition, contractors security clearance information is maintained by the COR
and the Contractor's Program Manager. Again, the COR was not interviewed by
the auditing team.

2

AFRC-CII
SUBJECT: Report on DoD Organization Information Assurance Management of
Information Technology Goods and Services Acquired Through Interagency
Agreements (Project No. D2005-D000AS-0173)

7. For further information contact Mr. Tom Blackburn, USARC, IAPM at
678-364-8246.

CHARLES E. PHILLIPS, JR.
Colonel, GS
Deputy Chief of Staff, G2/6

3

Department of the Navy Comments

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
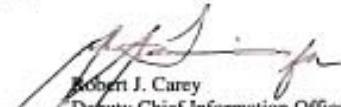WASHINGTON, DC 20350-1000

31 January 2006

From: Department of the Navy Chief Information Officer
To: Inspector General Department of Defense

Subj: DEPARTMENT OF DEFENSE INSPECTOR GENERAL DRAFT REPORT, "DOD
       ORGANIZATION INFORMATION ASSURANCE MANAGEMENT OF
       INFORMATION TECHNOLOGY GOODS AND SERVICES ACQUIRED THROUGH
       INTERAGENCY AGREEMENTS," PROJECT NO. D2005-D000AS-0173, OF
       6 JANUARY 2006

Encl: (1) Commander, Space and Naval Warfare Systems Command ltr 7502, Ser 00G/001 of
          23 Jan 06

       Enclosure (1) is endorsed and forwarded. If you have any questions, please contact
Mr. Dale Christensen at (703) 602-6800.

Robert J. Carey
Deputy Chief Information Officer for
Policy and Integration

DEPARTMENT OF THE NAVY
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
4301 PACIFIC HIGHWAY
SAN DIEGO, CA 92110-3127

7502
Ser 00G/001

JAN 2 3 2006

From: Commander, Space and Naval Warfare Systems Command
To: Inspector General Department of Defense

Subj: DODIG DRAFT REPORT "DOD ORGANIZATION INFORMATION ASSURANCE
      MANAGEMENT OF INFORMATION TECHNOLOGY GOODS AND SERVICES
      ACQUIRED THROUGH INTERAGENCY AGREEMENTS" (PROJECT NO. D2005-
      D000AS-0173) DATED 6 JANUARY 2006

Encl: (1) Space and Naval Warfare Systems Command Consolidated Response to
          Recommendations in Subject DoDIG Draft Report

1.   This is the Space and Naval Warfare Systems Command response to subject DoDIG report.
We have reviewed the draft report and provided our comments at Enclosure (1).

2.   Questions concerning this correspondence may be directed to Mr. John Gampel, Acting
Inspector General, at (619) 524-7065 or DSN 524-7065.

R.F. SMITH
Deputy Commander

**SPACE AND NAVAL WARFARE SYSTEMS COMMAND RESPONSE TO
RECOMMENDATIONS IN DRAFT AUDIT REPORT DATED 6 JANUARY 2006 ON
"DOD ORGANIZATION INFORMATION ASSURANCE MANAGEMENT OF
INFORMATION TECHNOLOGY GOODS AND SERVICES ACQUIRED THROUGH
INTERAGENCY AGREEMENTS" (PROJECT NO. D2005-D000AS-0173)**

We would like to reiterate, as stated in our 16 December 2005 response to the discussion draft provided on 14 December 2005, that the seven contractors referenced in the draft report were under the cognizance of SPAWAR Systems Center (SSC) San Diego. SSC San Diego confirmed that the seven contractors were their responsibility.

Recommendation 2: The DoDIG recommended that the Commander, Space and Naval Warfare Command direct the Chief Information Officer, Space and Naval Warfare Command and the Chief Information Officer, Space and Naval Warfare Systems Center Command, San Diego to:

a. Conduct and document annual information assurance awareness training, in accordance with DoD Directive 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, for all Space and Naval Warfare Systems Command employees and contractors.

Response: Space and Naval Warfare Systems Command (SPAWARSYSCOM), often referred to as SPAWAR Headquarters in the draft report, and SSC San Diego concur and are complying.

SPAWARSYSCOM and SSC San Diego both conduct user training and tracking compliance. This is documented in our recent compliance reports to the Naval Network Warfare Command (NNWC) where SPAWAR (as a claimancy) exceeded the 98 percent training requirement.

SPAWARSYSCOM currently conducts and documents annual Information Assurance (IA) awareness training for all military and government employees, and those contractors with computer system and network access. SPAWARSYSCOM works within the Navy Marine Corps Intranet (NMCI) network, which does not have the ability to electronically track training completion. In response to an NNWC and DON CIO mandate, SPAWARSYSCOM conducted command wide training in FY 2005, but was not provided with an electronic method for managing completion. Currently, a manual process is in place where individuals provide completion certificates to the Command Information Assurance Manager (IAM). All new personnel requiring access to NMCI via a SPAWARSYSCOM-sponsored account must complete training and provide a completion certificate to the IAM prior to receiving access approval. SPAWARSYSCOM is following NNWC and DON CIO progress on efforts to provide an automated process for tracking IA awareness training at the Navy Enterprise level.

SSC San Diego currently conducts and documents annual IA awareness training for all military and government employees, and those contractors with computer system and network access. SSC San Diego has an existing Access database, which does have the ability to

<div align="right">Enclosure (1)</div>

electronically track training completion. A web based training module has been established that automatically updates and tracks the individuals who complete the training. Training is recorded via SSC San Diego's corporate database with the individual's name and date of completion. Annual notification is automatically generated and sent via email to the individual 30 days prior to their anniversary date. Center-wide FY 2005 IA training was completed on 30 September 2005.

b.   Within 30 days of report issuance, establish clear procedures designating organization-specific roles and responsibilities for tracking training for all employees and contractors.

Response: SPAWARSYSCOM believes that it currently has a clear procedure and is complying. IAMs are appointed in writing for each command/system center within the claimancy. This appointment requires that the IAMs meet the roles and responsibilities outlined in SPAWAR Instruction 5239.1 "Information Assurance Program" dated 10 May 2005. This instruction clearly delineates the roles and responsibilities at Enclosure 1 "Roles and Responsibilities", Paragraph 1.e(6), which states, "The IAM shall...Ensure IS users receive annual IA awareness training and privileged users receive appropriate IA training." The IAM for each command/systems center within the claimancy is responsible for ensuring training of individuals with access to his/her network.

The SPAWAR Claimancy IA staff, including SSC San Diego, provides metrics to the Claimant IA Program Manager on a monthly basis, and holds monthly and quarterly program reviews where they address progress on key areas, such as compliance with training requirements.

c.   Within 30 days of report issuance, establish clear procedures designating specific roles and responsibilities for verifying individual security clearances in accordance with the Office of Management and Budget Circular A-130, "Security of Federal Automated Information Resources," November 28, 2000, for all Space and Naval Warfare Command employees and contractors.

Response: Concur. SPAWARSYSCOM will develop a policy directive to establish clear procedures for verifying individual personnel security clearances and clearly identify specific roles and responsibilities. The SPAWARSYSCOM Security Director will coordinate this policy with the SPAWARSYSCOM IA Manager. This policy directive shall cover the SPAWARSYSCOM claimancy to include supported PEOs.

Estimated date for completion is 30 June 2006.

d.   Begin using the Joint Personnel Adjudication System immediately to validate individual security clearances in accordance with the Office of the Under Secretary of Defense Memorandum, "Facilitating Classified Visits within the Department of Defense," April 1, 2005.

Response: Concur. SPAWARSYSCOM and SSC San Diego are in the process of implementing this requirement in accordance with the Office of the Under Secretary of Defense Memorandum, "Facilitating Classified Visits within the Department of Defense," April 1, 2005.

The SPAWARSYSCOM Security Director will hold an off site meeting with Site Security Directors during the 7-9 March 2006 DoD Security Conference. The Security Functional Change Lead (FCL) Team will address the issue of utilizing JPAS to send/receive official visit requests; identify resources required to perform this function; ensure compliance with Office of the Under Secretary of Defense Memorandum and Chief of Naval Operations (CNO) policy regarding classified visits to ensure visitor's identity and security clearance information is verified prior to authorizing access to SPAWAR facilities and to the classified information. The FCL Team will identify requirements, costs, and establish command policy, which will be incorporated in the new Security Policy directive/manual.

Estimated date for completion is 1 April 2006.

3   Enclosure (1)

Department of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE SECRETARY

26 Jan 06

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDITING
OFFICE OF THE INSPECTOR GENERAL

FROM: SAF/XC
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: DoD Organization Information Assurance Management of Information Technology Goods and Services Acquired Through Interagency Agreements, January 6, 2006 Project No. D2005-D000AS-0173

1. This memo is in reply to your memorandum requesting the Air Force comments on subject report.

2. The AEF Center Commander (AEFC/CC) concurs with the audit results and recommendation and has taken the following actions in accordance with AFI 65-402.

    a. The AEFC/CC ordered all inactive, suspended, or terminated accounts be deactivated immediately. The AEFC System owners implemented this order and completed all related actions on 13 Jan 06. Additionally, the system developers created an automated script to detect and disable any AEFC system accounts not accessed within the past 120 days.

    b. The AEFC/CC ordered weekly reviews of all system access logs under the control of the AEFC. Periodic reviews of system access logs will be performed and annotated in a System Information Assurance (IA) Log weekly. The System IA Log and basic interim procedures were created and implemented on 11 Jan 06. Permanent, more detailed procedures will be established and documented to ensure the review of AEFC system access logs is accomplished and recorded weekly (ref 2(c) below). Actions in response to DoD IG audit recommendations 3(b) and 3(c) will be completed concurrently.

    c. The AEFC/CC ordered development of permanent policy and procedures for monitoring user activity. This document will clearly communicate AEFC policy and fully detail procedures for monitoring user activity and establish a schedule for reviewing system access logs to ensure periodic reviews are accomplished and documented weekly by AEFC system managers. Document is due to AEFC/CC for approval on 15 Feb 06.

3. These recommendations have been coordinated with ACC/FMFPM and ACC/A6IA.

4. My POC is Col Gary Klabunde, SAF/XCIA, DSN 425-1511. The AEFC POC is Lt Col Michael Harbison, AEFC/AEPI, at DSN 575-4463.
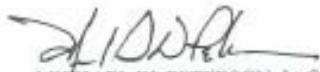
MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

cc:
AEFC/CC
SAF/PA
SAF/LL
SAF/IGI
AF/IL
AFAA/CC
ACC/FM
ACC/A6

2

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Acquisitions and Contract Management prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Mary L. Ugone
Richard B. Jolliffe
Jacqueline Wicecarver
Sean Davis
Therese Kince
Deirdre Beal
Benita Holliman
Kelly Lesly
Mandie Marr
Marcia Hart
Karma Cleveland
Matt Price
Meredith DePalma
Dana Fink
Jacqueline Pugh
Meredith H. Johnson